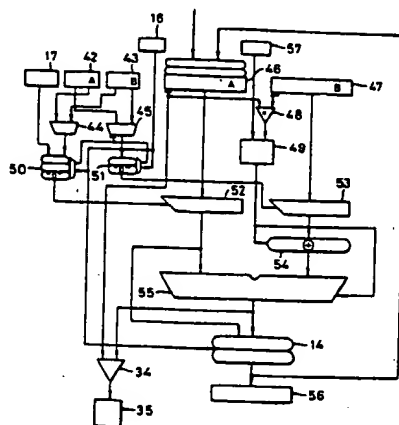


(54) DIGIT MATCHING CIRCUIT FOR DIVISION OPERAND

(11) 3-68020 (A) (43) 25.3.1991 (19) JP
 (21) Appl. No. 64-204056 (22) 7.8.1989
 (71) NEC CORP(1) (72) TAKASHI KANAZAWA(1)
 (51) Int. Cl.⁵ G06F7/52

PURPOSE: To efficiently execute the digit matching processing of an operand of a floating point division by adding some hardware to a floating point adding circuit.

CONSTITUTION: When a digit matching mode register 16 is in a regular mode, a result selector 14 always selects an output of an adder 55, and shift counting selectors A 50, B 51 execute all the same operation as a conventional circuit. When the digit matching mode register 16 is in a digit matching mode of a division operand, the result selector 14, the shift counting selector A 50, and the shift counting selector B 51 always output the output of an equalizing shifter A 52, the output of a digit matching shift counting register 17, and "0", respectively. By using this constitution, digit matching is executed by a prescribed sequence, the result of comparison of an absolute value is stored in an indicator register 35 through an absolute value comparator 34, and the result of right shift is stored in a result register 56.



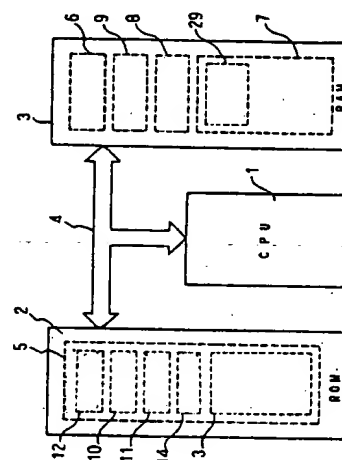
42: exponent A. 43: exponent B. 46: operand A. 47: operand B. 49: inversion instruction. 53: shifter

(54) ELECTRONIC COMPUTER

(11) 3-68023 (A) (43) 25.3.1991 (19) JP
 (21) Appl. No. 64-204096 (22) 7.8.1989
 (71) MITSUBISHI ELECTRIC CORP (72) MASANORI SATO
 (51) Int. Cl.⁵ G06F9/06, G06F9/40

PURPOSE: To suppress the reduction of reliability to the minimum by storing all loading programs in ROM, coupling a patch program on a RAM from an inlet position of a subroutine and executing it by a branch destination control program.

CONSTITUTION: A loading program 5 stored in ROM 2 is read successively through a bus 4, and brought to decoding processing by a CPU 1. A working area 6 on a RAM 3 is used as a storing place, a stacking area, etc., for a variable parameter and intermediate data under the control of the CPU 1. In the case of the regular execution, the loading program 5 executes an application program 13. Subsequently, by a program re-write requesting command of a ground station, a patch program writing program 12 and branch destination address writing program 10 are executed. Next, by the program 12, a patch program 29 is loaded on the space area 7 of the RAM 3.



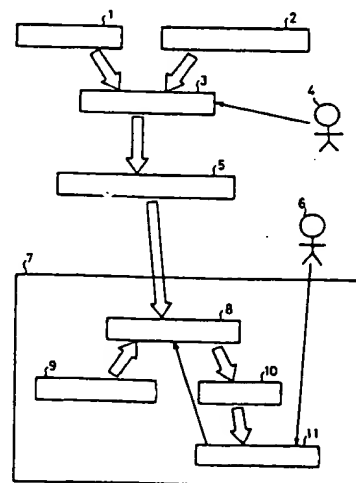
8: address table area. 9: breaking point flag area. 11: breaking point flag write program. 14: branch destination address writing program

(54) PREVENTING SYSTEM FOR ILLEGAL USE OF PROGRAM

(11) 3-68024 (A) (43) 25.3.1991 (19) JP
 (21) Appl. No. 64-204979 (22) 8.8.1989
 (71) NEC CORP (72) SHIGEYA MATSUO
 (51) Int. Cl.⁵ G06F9/06, G06F12/14

PURPOSE: To prevent a program from being used illegally for other system than a user system for which it is supplied by enciphering the program by using an encipherment key inherent to a program user system for which the program is supplied.

CONSTITUTION: In the case of supplying a program to a user system 7, a supplier 4 of the program prepares the program 1 supplied to the user system 7 and an intrinsic encipherment key 2, and actuates an enciphering means 3. The enciphering means 3 executes an encipherment by using the program 1 and the encipherment key 2 and generates a system intrinsic encipherment supplying program 5. In the case a user 6 executes the program 5, a program executing means 11 is actuated, and an enciphered program decoding means 8 is actuated. In such a manner, the decoding means 8 inputs the system intrinsic encipherment supply program 5 and a system intrinsic cipher decoding key 9, and outputs a decoding program 10.



⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A)

平3-68024

⑬ Int. Cl.³

G 06 F 9/06
12/14

識別記号

4 5 0 C
3 2 0 B

庁内整理番号

7361-5B
7737-5B

⑭ 公開 平成3年(1991)3月25日

審査請求 未請求 請求項の数 1 (全3頁)

⑮ 発明の名称 プログラムの不正使用防止方式

⑯ 特 願 平1-204979

⑰ 出 願 平1(1989)8月8日

⑱ 発 明 者 松 尾 篤 弥
⑲ 出 願 人 日本電気株式会社
⑳ 代 理 人 弁理士 境 廣 巳

東京都港区芝5丁目33番1号 日本電気株式会社内
東京都港区芝5丁目7番1号

明 細 書

1. 発明の名称

プログラムの不正使用防止方式

2. 特許請求の範囲

利用者システムに供給する供給プログラムと前記利用者システムに対する固有の利用者システム固有暗号化鍵とを入力して前記供給プログラムを暗号化したシステム固有暗号化供給プログラムを生成する供給プログラム暗号化手段を設けると共に、

前記利用者システムに、

前記システム固有暗号化供給プログラムと該システム固有暗号化供給プログラムを解読するためのシステム固有暗号解読鍵とを入力し、前記システム固有暗号化供給プログラムを解読した解読プログラムを生成する暗号化プログラム解読手段と、

該暗号化プログラム解読手段で解読された解読プログラムを実行するプログラム実行手段とを設けたことを特徴とするプログラムの不正使用防止方式。

3. 発明の詳細な説明

(産業上の利用分野)

本発明はプログラムの供給者がプログラムを供給した計算機システム以外でプログラムが使用されることを防止するプログラムの不正使用防止方式に関する。

(従来の技術)

従来、プログラムの供給者が利用者システムに供給するプログラムはそのままの形で利用者システムで実行可能なものであった。

(発明が解決しようとする課題)

従来は上述したように、そのまま実行可能な形で利用者システムにプログラムを供給するようになっているので、プログラムの供給者がプログラムを供給した利用者システム以外でもプログラムを実行することができる。このため、従来はプログラムの供給者がプログラムを供給した利用者システム以外で供給プログラムが不正使用されることを防止できないという問題があった。

本発明の目的はプログラムの供給者がプログラ

ムを供給したシステム以外で供給プログラムが不正使用されることを防止できるようにすることにある。

(課題を解決するための手段)

本発明は上記目的を達成するため、

利用者システムに供給する供給プログラムと前記利用者システムに対する固有の利用者システム固有暗号化鍵とを入力して前記供給プログラムを暗号化したシステム固有暗号化供給プログラムを生成する供給プログラム暗号化手段を設けると共に、

前記利用者システムに、

前記システム固有暗号化供給プログラムと該システム固有暗号化供給プログラムを解読するためのシステム固有暗号解読鍵とを入力し、前記システム固有暗号化供給プログラムを解読した解読プログラムを生成する暗号化プログラム解読手段と、

該暗号化プログラム解読手段で生成された解読プログラムを実行するプログラム実行手段とを設けたものである。

ム固有暗号化鍵 2 を入力してシステム固有暗号化供給プログラム 5 を生成する供給プログラム暗号化手段 3 と、利用者システム 7 内に設けられ、システム固有暗号化供給プログラム 5 及びシステム固有暗号解読鍵 9 を入力して解読プログラム 10 を生成する暗号化プログラム解読手段 8 と、解読プログラム 10 を実行すると共に暗号化プログラム解読手段 8 に起動指示を加えるプログラム実行手段 11 とを含んでいる。

供給プログラム暗号化手段 3 及び暗号化プログラム解読手段 8 はそれぞれ次式(1)、(2)に示す処理を行なう。

$$Q = P (P, K) \quad \dots\dots (1)$$

$$P = G (Q, L) \quad \dots\dots (2)$$

但し、式(1)、(2)に於いて、P は供給プログラム 1、K は利用者システム 7 に対する固有の利用者システム固有暗号化鍵 2、F は供給プログラム暗号化手段 3 の操作を示す関数、Q はシステム固有暗号化供給プログラム、G は利用者システム 7 の暗号化プログラム解読手段 8 の操作を示す関数、

(作用)

供給プログラム暗号化手段は利用者システムに供給する供給プログラムと利用者システムに対する固有の利用者システム固有暗号化鍵とを入力して供給プログラムを暗号化したシステム固有暗号化供給プログラムを生成する。利用者システムには暗号化プログラム解読手段とプログラム実行手段とが設けられ、暗号化プログラム解読手段はシステム固有暗号化供給プログラムとそれを解読するためのシステム固有暗号解読鍵とを入力し、システム固有暗号化供給プログラムを解読した解読プログラムを生成する。プログラム実行手段は暗号化プログラム解読手段で生成された解読プログラムを実行する。

(実施例)

次に本発明の実施例について図面を参照して詳細に説明する。

第 1 図は本発明の実施例のブロック図であり、利用者システム 7 に供給する供給プログラム 1 及び利用者システム 7 に対する固有の利用者システ

ムは利用者システム 7 固有のシステム固有暗号解読鍵 9 である。即ち、供給プログラム暗号化手段 3 は供給プログラム 1 と利用者システム固有暗号化鍵 2 とに対して関数 F で示される操作を行なって供給プログラム 1 を暗号化したシステム固有暗号化供給プログラム 5 を生成し、暗号化プログラム解読手段 8 はシステム固有暗号化供給プログラム 5 とシステム固有暗号解読鍵 9 とに対して関数 G で示される操作を行なってシステム固有暗号化供給プログラム 5 を解読し、元に戻した解読プログラム 10 を生成するものである。

次に本実施例の動作を説明する。

プログラムの供給者 4 は利用者システム 7 にプログラムを供給する場合、利用者システム 7 に供給する供給プログラム 1 及び利用者システム 7 に対して固有の利用者システム固有暗号化鍵 2 を用意し、供給プログラム暗号化手段 3 を起動する。供給プログラム暗号化手段 3 は起動されると、供給プログラム 1 と利用者システム固有暗号化鍵 2 とを入力し、供給プログラム 1 を利用者システム

固有暗号化鍵 2 を使って暗号化し、システム固有暗号化供給プログラム 5 を生成する。

利用者システム 7 の利用者 6 は供給者 4 によって供給されたシステム固有暗号化供給プログラム 5 を実行する場合、プログラム実行手段 11 を起動する。プログラム実行手段 11 は起動されると、暗号化プログラム解読手段 8 を起動する。これにより、暗号化プログラム解読手段 8 はシステム固有暗号化供給プログラム 5 とシステム固有暗号解読鍵 9 とを入力し、システム固有暗号化供給プログラム 5 をシステム固有暗号解読鍵 9 を使って解読し、供給プログラム 1 と同一の解読プログラム 10 を出力する。プログラム実行手段 11 は暗号化プログラム解読手段 8 から出力された解読プログラム 10 を実行する。

(発明の効果)

以上説明したように、本発明は、プログラムを供給しようとする利用者システム固有の利用者システム固有暗号化鍵を用いてプログラムを暗号化し、暗号化したプログラムを供給するようにした

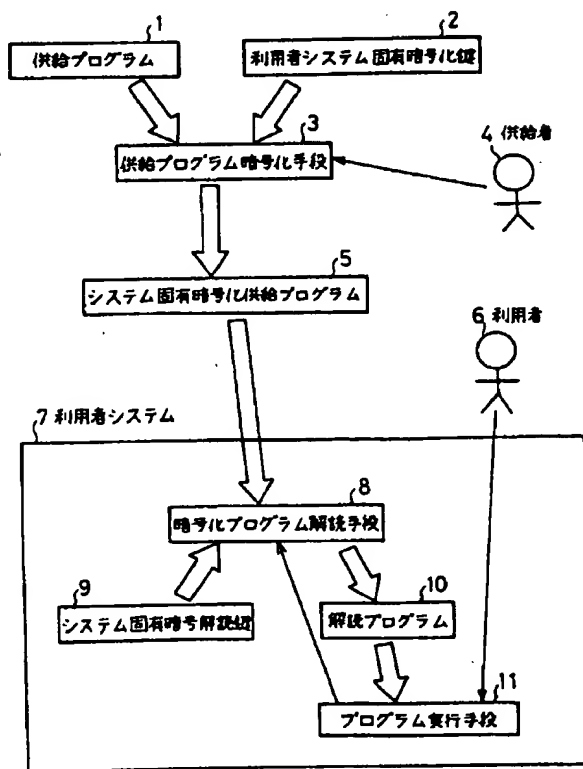
ものであり、プログラムの供給者がプログラムを供給した利用者システム以外ではシステム固有暗号解読鍵が不明であり、供給プログラムを解読、実行することができないので、プログラムの供給者がプログラムを供給した利用者システム以外でのプログラムの不正使用を防止することができる効果がある。

4. 図面の簡単な説明

第 1 図は本発明の実施例のブロック図である。

図に於いて、1…供給プログラム、2…利用者システム固有暗号化鍵、3…供給プログラム暗号化手段、5…システム固有暗号化供給プログラム、7…利用者システム、8…暗号化プログラム解読手段、9…システム固有暗号解読鍵、10…解読プログラム、11…プログラム実行手段。

特許出願人 日本電気株式会社
代理人 弁理士 境 廣 巳



本発明の実施例のブロック図

第 1 図